CLAIMS

What is claimed is:

1. A communication system comprising:

a communication network;

a server coupled to said communication network for determining a revocation status of a digital certificate in response to a status request;

a client coupled to said server through said communication network for transmitting said status request to said server, wherein a reply from said server to said client notifies said client of said revocation status; and

an on-line secure communication session over said communication network between said client and said server for securely transferring said reply automatically.

2. The communication system as described in Claim 1, wherein said digital certificate is associated with information requested by said client and transferred to said client by said server.

3. The communication system as described in Claim 1, wherein said client initiates an authentication protocol supported by a Secure Socket Layer (SSL) to authenticate said server in order to establish said secure communication session with said server.

4. The communication system as described in Claim 1, wherein said secure communication session is a Secure Socket Layer (SSL) communication session.

5. The communication system as described in Claim 1, further comprising:

a digitally signed certificate revocation list (CRL) accessed by said server to determine said revocation status of said digital certificate.

6. The communication system as described in Claim 5, wherein said CRL is maintained by said server so that said server can access the most current CRL.

7. The communication system as described in Claim 1, wherein said server sends a valid reply to said client over said secure communication session if said digital certificate has not been revoked, and sends an invalid reply to said client over said secure communication session if said digital certificate has been revoked.

8. The communication system as described in Claim 1, wherein said server loads a digitally signed certificate revocation list (CRL) upon startup, and authenticates said CRL, and assumes all digital certificates are revoked if said CRL cannot be authenticated.

9. The communication system as described in Claim 1, wherein said client polls said server for said information that is a software patch.

10. The communication system as described in Claim 1, wherein said status request is a Hypertext Transfer Protocol (HTTP) POST request.

11. A communication system comprising:

a communication network;

a server coupled to said communication network for determining a revocation status of a digital certificate in response to a status request associated with a poll for a software patch authenticated by said digital certificate;

a client coupled to said server through said communication network for initiating said poll and transmitting said status request to said server, wherein a reply from said server to said client notifies said client of said revocation status; and

an on-line secure communication session over said communication network between said client and said server for securely transmitting said reply automatically.

12. The communication system as described in Claim 11, wherein said client initiates an authentication protocol supported by a Secure Socket Layer (SSL) to authenticate said

server in order to establish said secure communication session with said server.

13. The communication system as described in Claim 11, wherein said secure communication session is a Secure Socket Layer (SSL) communication session.

14. The communication system as described in Claim 11, further comprising:

a digitally signed certificate revocation list (CRL) accessed by said server to determine said revocation status of said digital certificate, wherein said CRL is maintained by said server so that said server can access the most current CRL.

15. The communication system as described in Claim 11, wherein said server sends a valid reply to said client over said secure communication session if said digital certificate has not been revoked, and sends an invalid reply to said client over said secure communication session if said digital certificate has been revoked.

16. The communication system as described in Claim 11, wherein said server loads a digitally signed certificate revocation list (CRL) upon startup, and authenticates said CRL, and assumes all digital certificates are revoked if said CRL cannot be authenticated.

17. The communication system as described in Claim 11, wherein said status request is a Hypertext Transfer Protocol (HTTP) POST request.

18. The communication system as described in Claim 11, wherein said server transmits said reply before transmitting said software patch.

19. The communication system as described in Claim 11, wherein said server stores said information.

20. A method of validating a digital authentication comprising:

a) establishing a secure on-line communication session between a client and a server, wherein said client authenticates said server and requests status information of a digital certificate from said server over said secure communication session;

b) determining a revocation status of said digital certificate at said server in response to a status request from said client; and

c) notifying said client of said revocation status by securely transferring said revocation status to said client.

21. The method of validating as described in Claim 20, wherein c) further comprises:

securely transferring said revocation status prior to any transfer of information accessible by said server and authenticated by said digital certificate.

22. The method of validating as described in Claim 20, wherein a) further comprises:

requesting said status information when polling said server for information associated with said digital certificate; and wherein

b) and c) are performed automatically in response to said status request.

23. The method of validating as described in Claim 20, wherein said client authenticates said server through an authentication protocol supported by a Secure Socket Layer (SSL) that is initiated by said client when establishing said secure on-line communication session.

24. The method of validating a digital authentication as described in Claim 23, further comprising:

terminating said secure on-line communication session if said server is not authenticated.

25. The method of validating a digital authentication as described in Claim 20, wherein a) further comprises:

establishing said secure communication session to transmit said status request and a reply to said status request over said secure communication session.

26. The method of validating a digital authentication as described in Claim 20, wherein b) comprises:

checking said digital certificate against a digitally signed certificate revocation list (CRL).

27. The method of validating a digital authentication as described in Claim 26, further comprising:

maintaining said CRL by said server so that the most current CRL is accessible by said server.

28. The method of validating a digital authentication as described in Claim 20, wherein c) comprises:

sending a first reply over said secure communication session indicating said revocation status is valid from said server to said client, if said digital certificate has not been revoked; and

sending a second reply over said secure communication session indicating said revocation status is invalid from said server to said client, if said digital certificate has been revoked.

29. The method of validating a digital authentication as described in Claim 20, wherein c) comprises:

notifying said client of said revocation status with a reply without including a second digital certificate authenticating said reply over said secure communication session.

30. The method of validating a digital authentication as described in Claim 20, further comprising:

b) determining a second revocation status of a second digital certificate in response to a second status request from said client, said client requesting second information, said second information associated with said second digital certificate that authenticates said second information; and

c) notifying said client of said second revocation status of said prior to any transfer of said second information.

31. A method of validating a digital authentication comprising:

a) establishing a secure on-line communication session with a client for the transfer of a software patch to said client in response to a polling request for said software patch that is authenticated by a digital certificate;

b) determining a revocation status of said digital certificate in response to a status request from said client; and

c) notifying said client of said revocation status of said digital certificate prior to any transfer of said

software patch to said client over said secure communication session.

32. The method of validating as described in Claim 31, wherein said a), b), and c) are performed automatically.

33. The method of validating a digital authentication as described in Claim 31, wherein b) comprises:

checking said digital certificate against a digitally signed certificate revocation list (CRL).

34. The method of validating a digital authentication as described in Claim 31, wherein a), b) and c) are performed each time said client polls said server for the transfer of said software patch.

35. The method of validating a digital authentication as described in Claim 31, further comprising:

terminating said secure communication session if said revocation status indicates said digital certificate has been revoked; and

continuing said secure communication session if said revocation status indicates said digital certificate is valid.

36. The method of validating a digital authentication as described in Claim 31, wherein c) comprises:

sending a first reply over said secure communication session indicating said revocation status is valid from said server to said client, if said digital certificate has not been revoked; and

sending a second reply over said secure communication session indicating said revocation status is invalid from said server to said client, if said digital certificate has been revoked.

37. The method of validating a digital authentication as described in Claim 31, further comprising:

verifying said status request follows a prescribed format; and

sending a reply indicating said status request is bad if said status request does not follow said prescribed format.

38. The method of validating a digital authentication as described in Claim 37, further comprising:

terminating said secure communication session if said status request is bad.

39. The method of validating a digital authentication as described in Claim 31, further comprising:

before step b), loading a digitally signed certificate revocation list (CRL) at said server;

validating and authenticating said CRL; and

assuming all digital certificates are invalid if said CRL is invalid.

40. The method of validating a digital authentication as described in Claim 31, wherein c) comprises:

notifying said client of said revocation status with a reply without including a second signature validation on said reply over said secure communication session.